This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (original) A method for authorizing requested processing by an adjunct program module, the method comprising:

receiving a request from a requesting module;

receiving a certificate from the requesting module;

determining whether the certificate authorizes processing in response to the request; and

processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

2. (currently amended) The method of Claim 1 wherein determining ~~comprises: verifying a signature of the certificate by a certificate authority~~ whether the certificate authorizes processing includes determining whether the certificate has expired.

3. (original) The method of Claim 1 wherein determining comprises: determining that the requesting module owns the certificate.

4. (original) The method of Claim 3 wherein determining that the requesting module owns the certificate comprises:

sending test data to the requesting module; and

receiving response data from the requesting module wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

5. (original) The method of Claim 4 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

6. (original) The method of Claim 4 wherein the response data includes a cryptographic signature of the test data.

7. (original) The method of Claim 4 wherein the test data is encrypted according to the certificate.

8. (original) The method of Claim 7 wherein the test data is encrypted using a public key of the certificate.

9. (original) The method of Claim 7 wherein the response data is decrypted from the test data.

10. (original) The method of Claim 4 wherein determining further comprises: generating the test data randomly.

11. (currently amended) The method of Claim 1 wherein determining comprises:

determining that the certificate includes data specifying one or more types of actions permitted for the owner of ~~by~~ the certificate; and

determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

12. (currently amended) The method of Claim 1 wherein ~~the adjunct program module is a module in a dynamic link library~~ the certificate includes an owner field that identifies the owner of the certificate and wherein determining whether the certificate authorizes processing includes determining whether the requesting module owns the certificate.

13. (currently amended) A method for authorizing requested processing by an adjunct program module, the method comprising:

receiving a request from a requesting module;

receiving specified parameters from the requesting module including an authorization interface of ~~from~~ the requesting module and an authorization interface of an original requestor of the requesting module, if applicable;

requesting authorization from the requesting module according to the authorization interface;

receiving authorization data in response to the requesting authorization;

determining whether the authorization data authorizes processing in response to the request; and

processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

14. (currently amended) The method of Claim 13 wherein the authorization data includes a certificate owned by the original requestor of the requesting module.

15. (original) The method of Claim 14 wherein determining comprises: verifying a signature of the certificate by a certificate authority.

16. (original) The method of Claim 14 wherein determining comprises: determining that the requesting module owns the certificate.

17. (original) The method of Claim 13 wherein requesting authorization comprises:

sending test data to the requesting module; and

further wherein the authorization data includes response data wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

18. (original) The method of Claim 17 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

19. (original) The method of Claim 17 wherein the response data includes a cryptographic signature of the test data.

20. (original) The method of Claim 17 wherein the test data is encrypted according to the certificate.

21. (original) The method of Claim 20 wherein the test data is encrypted using a public key of the certificate.

22. (original) The method of Claim 20 wherein the response data is decrypted from the test data.

23. (original) The method of Claim 17 wherein sending test data further comprises:

generating the test data randomly.

24. (original) The method of Claim 13 wherein determining comprises:

determining that the authorization data includes data specifying one or more types of actions permitted by the certificate; and

determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

25. (original) The method of Claim 13 wherein the adjunct program module is a module in a dynamic link library.

26. (currently amended) A computer readable medium useful in association with a computer which includes a processor and a memory, the computer readable medium including computer instructions which are configured to cause the computer to authorize requested processing by an adjunct program module by:

receiving a request from a requesting module;

receiving a certificate from the requesting module, the certificate including an ownership field that identifies the owner of the certificate and an expiration field that identifies an expiration of the certificate;

determining whether the certificate authorizes processing in response to the request; and

processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

27. (currently amended) The computer readable medium of Claim 26 wherein determining comprises:

verifying that ~~a signature of~~ the certificate has not expired. ~~by a certificate authority~~.

28. (original) The computer readable medium of Claim 26 wherein determining comprises:

determining that the requesting module owns the certificate.

29. (original) The computer readable medium of Claim 28 wherein determining that the requesting module owns the certificate comprises:

sending test data to the requesting module; and

receiving response data from the requesting module wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

30. (original) The computer readable medium of Claim 29 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

31. (original) The computer readable medium of Claim 29 wherein the response data includes a cryptographic signature of the test data.

32. (original) The computer readable medium of Claim 29 wherein the test data is encrypted according to the certificate.

33. (original) The computer readable medium of Claim 32 wherein the test data is encrypted using a public key of the certificate.

34. (original) The computer readable medium of Claim 32 wherein the response data is decrypted from the test data.

35. (original) The computer readable medium of Claim 29 wherein determining further comprises:

generating the test data randomly.

36. (original) The computer readable medium of Claim 26 wherein determining comprises:

determining that the certificate includes data specifying one or more types of actions permitted by the certificate; and

determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

37. (original) The computer readable medium of Claim 26 wherein the adjunct program module is a module in a dynamic link library.

38. (currently amended) A computer readable medium useful in association with a computer which includes a processor and a memory, the computer readable medium including computer instructions which are configured to cause the computer to authorize requested processing by an adjunct program module by:

receiving a request from a requesting module;

receiving an authorization interface from the requesting module (the direct requestor) and any requestor of the requesting module (indirect requestor(s));

requesting authorization from the requesting module according to the authorization interface;

receiving authorization data in response to the requesting authorization;

determining whether the authorization data authorizes processing in response to the request; and

processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

39. (currently amended) The computer readable medium of Claim 38 wherein the authorization data includes a certificate owned by the original indirect requestor.

40. (original) The computer readable medium of Claim 39 wherein determining comprises:

verifying a signature of the certificate by a certificate authority.

41. (currently amended) The computer readable medium of Claim 39 wherein determining comprises: determining that at least one of the direct and indirect requestors ~~the requesting module~~ owns the certificate.

42. (original) The computer readable medium of Claim 38 wherein requesting authorization comprises:

sending test data to the requesting module; and further wherein the authorization data includes response data wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

43. (currently amended) The computer readable medium of Claim 42 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate <u>of the original requestor, whether a direct or indirect requestor</u>.

44. (original) The computer readable medium of Claim 42 wherein the response data includes a cryptographic signature of the test data.

45. (original) The computer readable medium of Claim 42 wherein the test data is encrypted according to the certificate.

46. (original) The computer readable medium of Claim 45 wherein the test data is encrypted using a public key of the certificate.

47. (original) The computer readable medium of Claim 45 wherein the response data is decrypted from the test data.

48. (original) The computer readable medium of Claim 42 wherein sending test data further comprises: generating the test data randomly.

49. (original) The computer readable medium of Claim 38 wherein determining comprises:

determining that the authorization data includes data specifying one or more types of actions permitted by the certificate; and

determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

50. (currently amended) The computer readable medium of Claim 38 wherein requesting authorization further includes requesting authorization data from each of the direct and indirect requestors. ~~the adjunct program module is a module in a dynamic link library~~.

51. (currently amended) A computer system comprising:

a processor;

a memory operatively coupled to the processor; and

a processing authorization module (i) which executes in the processor from the memory and (ii) which, when executed by the processor, causes the computer to authorize requested processing by an adjunct program module by:

receiving a request from a requesting module;

requesting authorization data from the requesting module (as a direct requestor) and any requestors of the requesting module (as indirect requestors);

receiving at least one ~~a~~ certificate from the direct and indirect requestors; ~~requesting module;~~

determining whether the certificate authorizes processing in response to the request; and

processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

52. (original) The computer system of Claim 51 wherein determining comprises: verifying a signature of the certificate by a certificate authority.

53. (currently amended) The computer system of Claim 51 wherein determining comprises: determining that at least one of the direct or indirect requestors ~~the requesting module~~ owns the certificate.

54. (currently amended) The computer system of Claim 53 wherein determining that at least one of the direct or indirect requestors ~~the requesting module~~ owns the certificate comprises:

sending test data to the requesting module; and

receiving response data from the requesting module wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

55. (original) The computer system of Claim 54 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

56. (original) The computer system of Claim 54 wherein the response data includes a cryptographic signature of the test data.

57. (original) The computer system of Claim 54 wherein the test data is encrypted according to the certificate.

58. (original) The computer system of Claim 57 wherein the test data is encrypted using a public key of the certificate.

59. (original) The computer system of Claim 57 wherein the response data is decrypted from the test data.

60. (original) The computer system of Claim 54 wherein determining further comprises: generating the test data randomly.

61. (original) The computer system of Claim 51 wherein determining comprises:

determining that the certificate includes data specifying one or more types of actions permitted by the certificate; and determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

62. (original) The computer system of Claim 51 wherein the adjunct program module is a module in a dynamic link library.

63. (currently amended) A computer system comprising:

a processor;

a memory operatively coupled to the processor; and

a processing authorization module (i) which executes in the processor from the memory and (ii) which, when executed by the processor, causes the computer to authorize requested processing by an adjunct program module by:

receiving a request from a requesting module, wherein the requesting module received the request from at least one prior requestor module, the request originating from an originating prior requestor module;

receiving an authorization interface from the requesting module;

requesting authorization from the requesting module regarding the originating prior requestor module; ~~according to the authorization interface;~~

receiving authorization data in response to the requesting authorization;

determining whether the authorization data authorizes processing in response to the request; and

processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

64. (currently amended) The computer system of Claim 63 wherein the authorization data includes a certificate owned by the original indirect requestor.

65. (original) The computer system of Claim 64 wherein determining comprises: verifying a signature of the certificate by a certificate authority.

66. (original) The computer system of Claim 64 wherein determining comprises: determining that the requesting module owns the certificate.

67. (original) The computer system of Claim 63 wherein requesting authorization comprises:

sending test data to the requesting module; and

further wherein the authorization data includes response data wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

68. (original) The computer system of Claim 67 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

69. (original) The computer system of Claim 67 wherein the response data includes a cryptographic signature of the test data.

70. (original) The computer system of Claim 67 wherein the test data is encrypted according to the certificate.

71. (original) The computer system of Claim 70 wherein the test data is encrypted using a public key of the certificate.

72. (original) The computer system of Claim 70 wherein the response data is decrypted from the test data.

73. (original) The computer system of Claim 67 wherein sending test data further comprises:

generating the test data randomly.

74. (original) The computer system of Claim 63 wherein determining comprises:

determining that the authorization data includes data specifying one or more types of actions permitted by the certificate; and

determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

75. (currently amended) The computer system of Claim 63 wherein an authorization provider of an intermediary prior requestor module forwards authority challenges from an authorization verifier of the adjunct program module to an authorization provider of the originating prior requestor module and forwards associated responses from the authorization provider of the originating prior requestor module to the authorization verifier of the adjunct program module to preserve authentication verification between the originating prior requestor module and the adjunct program module ~~is a module in a dynamic link library~~.

76. (new) The computer system of Claim 63 wherein an authorization provider of an intermediary prior requestor module requires authority verification by an authorization verifier of the originating prior requestor module as a prerequisite to providing the authorization data to an authorization verifier of the adjunct program module. to an authorization provider of the originating prior requestor module and forwards associated responses from the authorization provider of the originating prior requestor module to the authorization verifier of the adjunct program module to preserve authentication verification between the originating prior requestor module

77. (new) The computer system of Claim 76 wherein the authorization data includes a certificate owned by the original indirect requestor.

78. (new) The computer system of Claim 63 wherein each of the requesting modules and prior requestor modules, including the originating prior requestor module, includes an authorization provider adapted so that the behavior of the authorization providers can be modified without requiring modification to other elements of the respective requesting and prior requestor modules.

79. (new) The computer system of Claim 63 wherein each of the requesting modules and prior requestor modules, including the originating prior requestor module, includes an authorization interface adapted so that authorization code is supplied separately from substantive computer code of any of the respective modules.